An invitation to algebraic number theory and class field theory

Ruíz Duarte, Eduardo

An invitation to algebraic number theory and class field theory

Eduardo Ruiz Duarte (e.ruiz.duarte@rug.nl)
Rijksuniversiteit Groningen

March 1, 2017

Abstract

This informal document was motivated by a question here at my university by a bachelor student. I will try to expose something that personally I think is impressive. The aim is to do it in such a way that is understandable with a basic knowledge of algebra.
We will examine without any rigor the "generalization" in some sense of the concept of "factorization", not just in the integers $\mathbb{Z}$ but in some "generalized" integers from number fields of the form $\mathbb{Q}(\sqrt{-n})$ for $n > 0$ which are called imaginary quadratic number fields. The problems in these new rings that will arise will give us interesting mathematics.

Contents

First of all we will assume that the rings that we will use here are commutative and they will have a multiplicative neutral element 1.
We begin with basics, most of the people here are familiar with the ring of integers:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

We know that in $\mathbb{Z}$ are prime numbers and composite numbers.

Then we have the field $\mathbb{Q}$ with all the "fractions" in it gotten from numbers of $\mathbb{Z}$. In $\mathbb{Q}$ numbers like π, e are missing. There are just numbers that can be represented as $\frac{a}{b}$ such that $a, b \in \mathbb{Z}$.

The most usual ring of integers is of course $\mathbb{Z}$, but we can add a new algebraic element in it and experiment with this new space. For example if we add the root of a polynomial which is not rational (an algebraic number); and then we calculate all the possible combinations of it with the field $\mathbb{Q}$, we will get a new field.

For example if we adjoin one of the roots of $x^2 + 5$ which is $\sqrt{-5} = i\sqrt{5}$ where i is the imaginary unit we get the imaginary quadratic field:

$$\mathbb{Q}(\sqrt{-5}) = \{a + b\sqrt{-5} : a, b \in \mathbb{Q}\} \tag{1}$$

This space is like the usual $\mathbb{Q}$, but we added a new element not in $\mathbb{Q}$ (the algebraic number $\sqrt{-5}$). Is easy to see that every nonzero element there has inverse and that the product of two elements also belongs to $\mathbb{Q}(\sqrt{-5})$.
Take $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$ then the product of both numbers is given by $ac - 5bd + (ad + bc)\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$ and the inverse of $a + b\sqrt{-5}$ is given by:

$$\frac{1}{a + b\sqrt{-5}} = \frac{a}{a^2 + 5b^2} + \frac{-b\sqrt{-5}}{a^2 + 5b^2} \in \mathbb{Q}(\sqrt{-5})$$

So, $\mathbb{Q}(\sqrt{-5}$ is a well defined field, just as $\mathbb{Q}$.

The ring of integers which will be the equivalent to $\mathbb{Z}$ in $\mathbb{Q}$, but now for $\mathbb{Q}(\sqrt{-5})$ is:

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \tag{2}$$

Is well known that the usual ring of integers $\mathbb{Z}$ is a Unique Factorization Domain, this means that any number can be factored in prime numbers of $\mathbb{Z}$ in a unique way.

For a general number field (extensions of $\mathbb{Q}$ by other algebraic elements like our example) this is not always true, in our example $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

Example:

$$6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3}$$

So we will see what is happening here, but first we will need some theory, I begin with the essential, and finish with the deep theory.

0.1 Rings

We know that a general ring has two operations $\langle R, +, \cdot \rangle$ where with the addition $\langle R, + \rangle$ all elements have an additive inverse, a neutral element and here particularly is commutative. Also it has a product $\langle R, \cdot \rangle$ which interacts via the law of distributivity with the addition. Here in R not necessary every element is invertible.
The common example is again $\langle \mathbb{Z}, +, \cdot \rangle$ because the multiplicative inverse of the nonzero $a \in \mathbb{Z}$ is an integer $a^{-1} \in \mathbb{Z}$ such that $a \cdot a^{-1} = 1$, such number does not exist in $\mathbb{Z}$ unless $a = \pm 1$ because there is no $\frac{1}{a} \in \mathbb{Z}$ for $a \neq \pm 1$. For the addition for each integer a there is always a "negative" $-a$ such that under $+$ it gives us 0, this means $a + (-a) = 0$ (neutral element).

0.2 Ideals of a Ring

A ring $\langle R, +, \cdot \rangle$ is an algebraic structure that has some subalgebraic structures called **ideals**. If $I \subset R$ is an ideal then their elements form a group under $+$, namely $\langle I, + \rangle \leq \langle R, + \rangle$ and for $a \in I$ multiplication by every element $r \in R$, namely $a \cdot i \in I$, that is $aI = I$.

For example in $\mathbb{Z}$ consider the "multiples of n" there are the ideals and we denote them as $n\mathbb{Z} := \{n \cdot a : a \in \mathbb{Z}\}$.
The reason that $n\mathbb{Z}$ is closed under addition is rather obvious as $a, b \in n\mathbb{Z}$ implies that $a + b = n\alpha + n\beta = n(\alpha + \beta) \in n\mathbb{Z}$ for some $\alpha, \beta \in \mathbb{Z}$. The other property of the ideal is also obvious as for $r \in \mathbb{Z}$ and $a \in n\mathbb{Z}$ we have that $ra = n\alpha r \in n\mathbb{Z}$ for some $\alpha \in \mathbb{Z}$.

Said this, these ideals $I \subset R$ behave more-less like a vector space over R (an R-module), as $rI = I$ for all $r \in R$, just like in $\mathbb{R}^2$ which can be seen as a $\mathbb{R}$-vector space, as any element $v \in \mathbb{R}^2$, can be multiplied by an $\alpha \in \mathbb{R}$

such that $\alpha v \in \mathbb{R}^2$.
Note that if $1 \in I$ then $I = R$, so much more interesting examples arise when the ideal is not the ring, which is our case.

So now, we said that the ideals $I \subset R$ behave "like a vector space", well then we can think in a "basis" of them, which means, a set of elements that generate the ideal. This is denoted by $I = \langle a, b \rangle$ If you just need 1 element we call the ideal **principal**, that is $I = \langle a \rangle = aR$ for some $a \in R$.
In $\mathbb{Z}$ all ideals as principal.
So, now $\mathbb{Z}$ is starting to be boring, because an ideal of $\mathbb{Z}$ given by $\langle m, n \rangle$ consists in all the linear combinations $xm + yn$ and is generated by one element.
More precisely $\langle m, n \rangle = \langle \gcd(m, n) \rangle = \gcd(m, n)\mathbb{Z}$.

The proof that every ideal in $\mathbb{Z}$ is principal can be seen here for the curious `https://proofwiki.org/wiki/Ring_of_Integers_is_Principal_Ideal_Domain`.
Returning to our example with the ring of integers $\mathbb{Z}[\sqrt{-5}]$ of the field $\mathbb{Q}(\sqrt{-5})$, there are ideals, like $I = \langle 3, 1 + \sqrt{-5} \rangle$ that are not principal.

Principal ideals play a crucial role in unique factorization of R as we will see in the next theorem.

Theorem 1:
Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field and R its ring of integers, then: All ideals of R are principal if and only if R has unique factorization for its elements.

We will prove in the next section that $I = \langle 3, 1 + \sqrt{-5} \rangle$ is not principal and hence, using the latter theorem $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. We already knew that it was not a factorization domain as 6 as an element of $\mathbb{Z}[\sqrt{-5}]$ has two different non trivial factorizations.

The next section can be skipped as it has more technicalities, but is just to fill a big hole that a curious person may find in this informal text.

0.3 Proving that an ideal of a ring of integers is not principal

Recall that this is informal, so I will give the essential ideas.
The basic tool to factorize in the ring of integers $\mathbb{Z}[\sqrt{D}]$ (where D is non

square) is the following:

Definition: *The norm of a quadratic field of the form* $\mathbb{Q}(\sqrt{D})$ *for a non-square* D *is given by the function* $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ *such that:*

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

The following property is the key of why the norm is important to factorize when applied to elements $\mathbb{Z}[\sqrt{D}]$.

Proposition 2: *Let* $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$ *then if* N *is its associated norm then* $N(\alpha\beta) = N(\alpha)N(\beta)$.

Now using this proposition the next theorem tells us information about the "dimension" of the ideal of a number field in general, i.e. the number of generators of the ideal.

Theorem 3: *Let* R *be a ring of integers of a number field* K*, consider* $z \in R$ *and the principal ideal generated by* z*, namely* $(z) = zR$ *then* $N(z) = \#R/(z)$

With this theorem 3 now we can prove something about the factorization of the integers in $K = \mathbb{Q}(\sqrt{-5})$ when we combine it with theorem 2. So here $R = \mathbb{Z}[\sqrt{-5}]$ and $N(a + b\sqrt{-5}) = a^2 + 5b^2$.
We want to prove that $I = \langle 3, 1 + \sqrt{-5}\rangle$ is not principal. So using the previous theorem this reduces to prove that $\#R/I \neq N(z)$ for all $z \in R$. This is easy as $R/(3) \cong \mathbb{Z}/3\mathbb{Z}[\sqrt{-5}]$ then $\#R/(3) = 9$ and this implies that for the quotient with the bigger ideal I we have $\#R/I = 3$, then we would like an element $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ with norm 3, which means we want an integer solution to $a^2 + 5b^2 = 3$ which is impossible. and then I cannot be principal.

0.4 Operations with ideals of a ring

Consider now set of all ideals $I \subseteq R$ (counting the trivial ideal R), call them $\mathfrak{I}$, now if you take $I, J \in \mathfrak{I}$ there is a way of multiply them $K = I \otimes J$ in such a way that $K \in \mathfrak{I}$, that is, K is also an ideal of $\langle R, +\cdot, \rangle$.
We define

$$I \otimes J := \left\{ \sum_{i=1}^{n} a_i \cdot b_i : a_i \in I, b_i \in J \ \forall n \in \mathbb{N} \right\} \tag{4}$$

This new ideal $I \otimes J$ is intuitively all the possible products ab that can be constructed for $a \in I$ and $b \in J$.

Example: Consider the ring of polynomials in 4 variables with complex coefficients $R = \mathbb{C}[x, y, z, w]$ and consider the following ideals generated by different combinations of variables $I = (z, w),\ J = (x+z, y+w),\ K = (x+z, w)$. Then:

$$IJ = (z(x+z), z(y+w), w(x+z), w(y+w)) = (z^2 + xz, zy + wy, wx + wz, wy + w^2)$$
$$IK = (xz + z^2, zw, xw + zw, w^2)$$

Now we need to drop redundant ideals in $\mathfrak{I}$ so we define an equivalence relation $\sim$ in the ideals of $\mathfrak{I}$, namely $I \sim J$ if there are $a, b \in R$ such that $aI = bJ$. So here, ideals which are related by $\sim$ are denoted as $[I]$. If you choose a representative of $[I]$ and $[J]$ then $[I] \otimes [J] = [IJ]$ is well defined and commutative.
So here we have a new structure $\mathfrak{I}/\sim$ which has multiplicative structure with the ideals.

0.5 Extending the ideals to fractional ideals

Here comes an interesting part, we are limiting ourselves to rings of the form $\mathbb{Z}[\sqrt{D}]$ for a non square D which are the integers of the quadratic field $\mathbb{Q}(\sqrt{D})$.
Now we would like to define for an ideal $I \subset \mathbb{Z}[\sqrt{D}]$ another ideal I^{-1} which we will call fractional Ideal, that will give us an "identity", the identity will be the boring ideal we mentioned before, which is the whole R. So we are trying to find a good structure for I^{-1} such that $I \oplus I^{-1} = R$.

This I^{-1} will depend now in the elements of $\mathbb{Q}(\sqrt{D})$, as we need some "fractions", to "clear" denominators and get the $1 \in I \otimes I^{-1}$ which makes an ideal trivial, i.e. it makes it R.

$$I^{-1} := \{z \in \mathbb{Q}(\sqrt{D}) : z \cdot I \subseteq \mathbb{Z}[\sqrt{D}]\}$$

This is exactly as we need, as the z are the "fractions" in the fields where multiplied by I stays in the integer ring $\mathbb{Z}[\sqrt{D}]$. Then we have that $I \otimes I^{-1} = R$.

This fractional ideals are not exactly ideals of $\mathbb{Z}[\sqrt{D}]$ as they are not elements of $\mathbb{Z}[\sqrt{D}]$, they are $\mathbb{Z}[\sqrt{D}]$-submodules of the field $\mathbb{Q}(\sqrt{D})$ but this

is a matter of terminology.

A big remark is that for a general integer ring R is not always possible to invert the ideals, but in our world of number fields $\mathbb{Q}(\sqrt{\alpha})$ where α is an algebraic integer, the ideals of the corresponding integer ring are **always** invertible.

Here we are studying **Dedekind Rings** which means that every ideal $I \subset \mathbb{Z}[\sqrt{D}]$ can be factored by prime ideals using the multiplication $\otimes$. This means that it is always possible to find a **unique finite set** of prime ideals $\{P_i\}$ of $\mathbb{Z}[\sqrt{D}]$ such that $I = \bigotimes P_i$.

0.6 Class group of a ring of integers

The final object is built from the multiplicative structure given before, namely by all the ideals $I \subseteq R$ with the equivalence relation $\sim$, and with multiplication of ideals $\otimes$ namely $\langle \mathfrak{I}/\sim, \otimes \rangle$.
Now extend $\mathfrak{I}/\sim$ to all the fractional its ideals (we can do this as we are supposing that R is a Dedekind domain), call this extension to fractional ideals $\mathfrak{F}$.
Consider now the same equivalence clases of $\mathfrak{F}$ using $\sim$ defined in the previous section.
We define the Class group of R by

$$\mathrm{Cl}(R) := \langle \mathfrak{F}/\sim, \otimes \rangle \tag{5}$$

Theorem 4: *Let R be a ring of integers of a number field K then $\#Cl(R) = 1$ if and only if R has unique factorization*

0.7 Weird and impressive facts about Cl(R) and conclusion

The class group $\mathrm{Cl}(R)$ as the theorem 4 says, has only 1 element then the ring R has unique factorization in its elements (not only on ideals), so it measures in some way how complicated the factorization behaves in a ring R.
A Weird and impressive thing is that for rings of the form $\mathbb{Z}[\sqrt{-n}]$ there is only a finite number of values for n where $\mathbb{Z}[\sqrt{-n}]$ has Unique factorization of its elements (not only in on the ideals). This is the same as saying

that $\#\mathrm{Cl}(\mathbb{Z}[\sqrt{-n}]) = 1$ by theorem 4. The numbers for n such that we get Unique factorization are: $\{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.
These weird numbers that generate Unique factorization in their associated imaginary quadratic fields are called **Heegner numbers**, and our example $\mathbb{Z}[\sqrt{-5}]$ as we saw does not have Unique factorization as 5 is not a Heegner number, and in fact $\#\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = 2$.

These Heegner numbers also are related to something that could be a mathematical coincidence but, it isn't, and is the fact that the numbers $e^{\pi\sqrt{43}}, e^{\pi\sqrt{67}}, e^{\pi\sqrt{163}}$ are "almost an integer":

$e^{\pi\sqrt{43}} \approx 884736743.999777466$
$e^{\pi\sqrt{67}} \approx 147197952743.999998662454$
$e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999925007$

This is not a coincidence but proving it, requires a little more analytic theory and the theory of Eisenstein series, but I hope this move your mind to be more interested in algebraic number theory.